ON EFFICIENT AND SECURE MODIFIED BUYER-SELLER WATERMARKING PROTOCOL

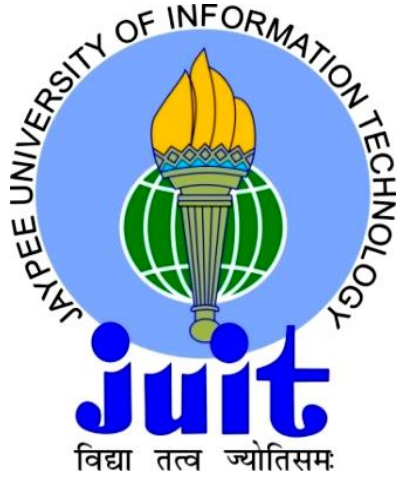
Synopsis submitted in fulfillment of the requirements for the Degree of

DOCTOR OF PHILOSOPHY

By

ASHWANI KUMAR

Enrollment No. 126204



Under the supervision of

Prof. S.P Ghrera

Dr. Vipin Tyagi

Department of Computer Science and Engineering

JAYPEE UNIVERSITY OF INFORMATION TECHNOLOGY, WAKNAGHAT

April, 2016

ABSTRACT

The rapid growth of internet and e-commerce needs a copyright protection mechanism for multimedia information. Buyer-Seller watermarking protocol (BSWP) is used to extend the digital rights of both the purchaser and the vendor. Although in that respect are many published articles on buyer-seller watermarking protocol, but still many problems to be solved in the buyer, seller watermarking protocol such as if we resolve the customer's right problem then unbinding will occurs. If we employ a double watermark insertion technique, conspiracy problem will occurs. In this synopsis, the author has concentrated on managing the watermarks means the business is only watermark insertion protocol and watermark extraction protocol and made out his research in this focal point in order to get to the watermarking embedding and extracting algorithm more robust, imperceptible and improve the optical appearance of watermarked images. The existing buyer-seller watermarking protocol uses some traditional methods for embedding and extracting the watermark. These methods were not robust and efficient for embedding the watermark into the original digital content. The author has proposed a robust and efficient watermarking embedding and extraction system based on discrete wavelet transform to improve the robustness and imperceptibility of the watermark.

Further, the author has offered a lightweight watermarking embedding and extraction scheme as an improved variation of the above scheme which makes purpose of principal component analysis with wavelets together for further increasing the validity of the watermark. The buyer seller digital watermarking protocol basically depends upon the underline cryptosystems and digital watermarking techniques. Previously, the author has figured out on digital watermarking schemes which embed the watermark into original digital content and improve the validity of the watermark and imperceptibility of digital content. Here, the author has worked on a cryptosystem because traditional cryptosystem did not explain much about how a watermark is generated, embedded, and detected. For that author used Id-based public key cryptography with digital watermarking systems for both the purchaser and the vendor. To check the imperceptibility and robustness of the watermarked image, PSNR and NCC parameters are used. Furthermore, the proposed algorithm is robust against the various attacks such as JPEG Compression, Rotation, Gaussian Noise, Median Filter and Salt & Pepper Noise.

Table of Contents

	PAGE NO.
ABSTRACT	ii
1. INTRODUCTION	4
1.1. Buyer-seller watermarking protocol	5
1.2. Problem identification	8
1.3. Objectives of thesis	8
1.4. Organization of thesis	9
2. OBJECTIVE	
2.1 Objective – 1	11-15
2.2 Objective – 2	16-18
2.2 Objective – 3	19-22
3. CONCLUSION	23
4. REFERENCES	25-28
5. LIST OF PUBLICATIONS	29

1. INTRODUCTION

The speedy development of internet and e-commerce needs a copyright protection mechanism for multimedia data. Straight off a day's digital watermarking becomes an important technique for protecting the digital rights [1]. This hidden information can subsequently be taken out to prove the ownership of the digital content [2]. With the increasing use of the internet, there is always a need to protect the multimedia data over the network. Data hiding in still images has two main applications such as fingerprinting and copyright protection. But important aspects of digital watermarking systems include imperceptibility, robustness, capacity and security of the embedding and extracting process.

Digital multimedia has become innovative in the field of internet application and data securities because copyright protection and data integrity detection has become a vast concern. The research in the area of digital watermarking has focused on the design of robust and secure watermarking techniques for piracy tracing and copyright protection of multimedia content. Copyright marking [3] is a relatively a new technique for hiding information in multimedia content with the aim of tracing any traitor who redistributes the digital content illegally.

The principal object of digital watermarking technique is to retain digital copyright or watermark, embedded into the cover object. The desirable secure digital watermarking scheme is one, which integrates public key cryptosystem and digital watermarking technique for protecting the buyer and marketer in a digital content transaction. Digital watermarking [4] techniques use encrypted domain for embedding and extracting the watermarks. The rapidly growing of the internet encourages some bad usage too, similar operations such as transformation, duplication, and redistribution of digital content. With the accessibility of some software tools, we can easily identify these bad users and redistribution of digital capacity can also be identified. Even though we stress to protect digital content from unauthorized access and manage its use rights. No matter how secure the access control mechanism. Digital content eventually needs to be confronted in the clear to the viewing audience.

In general, secure digital watermarking [5] scheme should satisfy the following requirements.

- **Robustness:** The capability of watermark to resist various image processing attacks such as rotation, scaling, clipping etc.
- **Imperceptibility:** The optical distortion of the watermarked image should not have on the quality of the original painting.
- **Effectiveness:** The algorithms for embedding and extracting the watermark into the digital content should be effective.
- **Fingerprinting:** A fingerprinting technique can be used to trace the source of illegal copy. Every copy available can be watermarked with a unique number sequence.

1.1. BUYER-SELLER WATERMARKING PROTOCOL

The buyer-seller watermarking protocol utilize watermarking along with cryptography for copyright and copy protection for the seller and at the same time it also preserves the buyer's rights to privacy. The buyer–seller watermarking protocol [6-14] is a three-party protocol among a service provider (seller), a customer (buyer) and a trusted watermark certificate authority (WCA). The buyer-seller watermarking protocol [15-19] is one that combines encryption and digital watermarking techniques to ensure rights protection for the buyer and the seller in e-commerce. A buyer-seller watermarking protocol [20] is expected to resolve the following problems:

- Certification authority obligation problem- This problem happens in existing watermarking protocols. The problem is to provide a digital certificate for both buyer and seller. A seller may fabricate piracy to frame the buyer.
- Conspiracy problem- Malicious parties collude with each other and mount attacks to frame a buyer or to confound the tracing by removing the water line from the digital content.
- Copy detection problem- Pirated copy of content or data must be detectable and traceable back to the owner of the original copy.
- Customer’s rights problem- If seller attempt to frame an innocent buyer, the seller may make and distributed a copy of X which the buyer has purchased. Then the seller may accuse the buyer for the illegal distribution of digital content.

- Piracy tracing problem- when a pirated copy is found, an innocent seller should be able to discover the pirated copy. The seller should be able to trace and identify the copyright violator.
- The unbinding problem- Unable to bind a watermark to particular digital content or transaction. The seller may distribute pirated by transplanting the buyer's watermark into other contents.

The whole process of buyer, the seller watermarking protocol is given below.

1. Requesting for a valid watermark to the WCA
2. Returning the generated watermark back to the buyer
3. Sending out the purchase order to the seller
4. Making the delivery back to the buyer

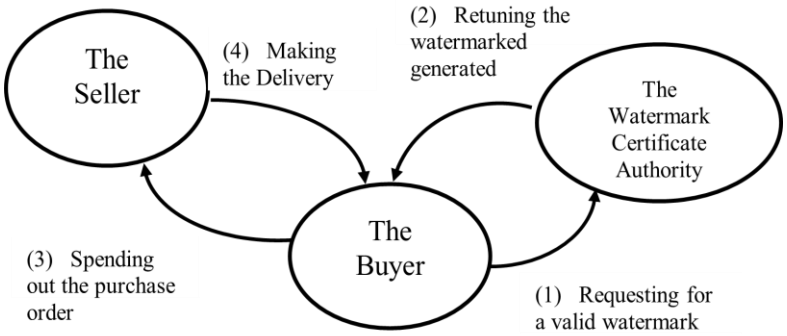

The Seller
(4) Making the Delivery
(2) Retuning the watermarked generated
The Watermark Certificate Authority
The Buyer
(3) Spending out the purchase order
(1) Requesting for a valid watermark

Fig. 1. *Interactions among the buyer, the seller, and the watermark certification authority [21]*

A buyer-seller watermarking protocol consists four main sub-protocols, i.e. Watermark generation protocol, Watermark insertion protocol, Copyright violator identification protocol and Dispute resolution protocol as presented in figure 2.

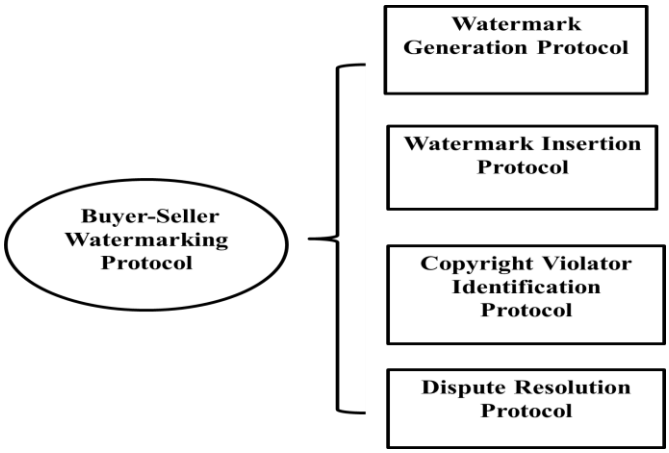


Fig. 2. *Four sub-protocols that comprise the buyer- seller watermarking protocol (BSWP) [21]*

A. Watermark Generation Protocol

The buyer sends a certification of his individuality and his public key to the trusted watermark certification authority (WCA) and requests a valid watermark. The watermark certification authority after establishing buyer's credentials generates a random but valid watermark and is sent to the buyer, the watermark encrypted with buyer's public key along with a digital signature sign that certifies the validity of the watermark.

B. Watermark Insertion Protocol

This is a two-party protocol between seller and buyer in which buyer sends to seller the encrypted watermark along with the signature sign of the watermarked certification authority. Seller verifies signatures in order to be assured that is indeed a valid watermark generated by watermarked certification authority.

C. Copyright Violator Identification Protocol

On discovering an unauthorized copy of seller can determine the buyer from whom this copy has originated by detecting the unique watermark that seller inserted for each buyer. This is done by means of a watermark extraction function which is depending on the watermarking technique. Using this extracted watermark buyer then locates in Table to whom was sold.

D. Dispute Resolution Protocol

In case buyer denies that an unauthorized copy has originated from his version of the image, then the seller can reveal and Sign to the judge. The judge first verifies signatures. He would then ask the buyer for his private key which he can compute and check for the presence of a watermark in unauthorized copy.

1.2. PROBLEM IDENTIFICATION

In this thesis, the author has focused on the design of robust and secure watermarking techniques for piracy tracing and copyright protection of multimedia content. In this research work, the author has focused on the following problems

1. *In the literature survey of BSWP author have found that the existing buyer-seller watermarking protocols are still not full filling the actual requirements of the user i.e. how to provide full freedom to the customers.*
2. *Some protocols are very good in comparison to others and some are the extended or modified versions of the other protocol.*
3. *So we need to discover more efficient & robust buyer, seller watermarking protocol, which takes less computational time and increase security, robustness, efficiency and flexibility.*
4. *The cryptosystem and digital watermarking scheme used by traditional BSWP are not much efficient.*
5. *For embedding and extracting the watermark the traditional buyer, seller watermarking protocol does not use the robust watermarking scheme.*
6. *The time taken by watermark insertion protocol and generation protocol can be reduces.*
7. *The security of this buyer-seller watermarking protocol lies on the security and robustness of the encryption standard and group signature techniques to improve the efficiency of the protocol.*

1.3. OBJECTIVES OF THESIS

Multimedia technology is buyer seller watermarking protocol which play important role in digital content distribution because it supports copyright information (such as the owner's identity, transaction dates, and serial numbers) for embedded as unperceivable signals into digital contents. Author’s purposed a modified buyer seller watermarking protocol which is secure and efficient which gives more security from the previous proposed protocol.

Objective of this thesis are

- To propose a robust and efficient watermarking embedding and extraction scheme based on discrete wavelet transform to improve the robustness and imperceptibility of the watermark.
- To propose a lightweight watermarking embedding and extraction scheme as an improved variation of the above scheme which makes use of principle component analysis with wavelets together for further increasing the robustness of the watermark.
- To propose a cryptosystem with digital watermarking scheme which uses id-based public key cryptography for providing more security to the buyer and seller. In this we also make use of a tamper resistance device to reduce the overhead on WCA as TTP.
- To propose a scheme in which time-stamp can be used by TTP to keep accountability of digital signature based on composite signal representation to provide a secure communication between buyer and seller.
- To propose an approach for supporting multi-transaction and dispute resolution and also avoid double watermark insertion.
- To propose such a digital watermarking scheme that have the ability to overcome the problem which were existing in previously published protocol and increase the efficiency as well as security between buyer and seller.

We have design a digital watermarking protocol with cryptographic technique to obtain the several objectives and identified number of problems in existing buyer seller watermarking protocol and their solutions are proposed.

1.4. ORGANIZATION OF THESIS

The synopsis has been organized as follows.

First, the authors have given the introductory part of the synopsis. Then authors have divided their research work into three different problems. The solutions of these problems are represented by three objectives. In the first objective, authors have presented a robust and efficient watermarking embedding and extraction scheme based on discrete wavelet transform to improve the robustness and imperceptibility of the watermark. In objective second, authors have presented a lightweight watermarking embedding and extraction scheme as an improved

variation of the above scheme which makes use of principle component analysis with wavelets together for further increasing the robustness of the watermark. Objective three presents a cryptosystem with digital watermarking scheme which uses id-based public key cryptography for providing more security to the buyer and seller. In this authors have presented a scheme in which time-stamp can be used by TTP to keep accountability of digital signature based on composite signal representation to provide a secure communication between buyer and seller. Then authors discussed conclusion and future scope of the research work. References and list of publications are given at the last of this synopsis.

1.5. SPECIFICATION OF THE SYSTEM:

PC configuration: Intel(R) Core(TM) 2 Duo CPU T6600, 2.20 GHz, 3 GB of RAM.

Operating System: Microsoft Window 7 Ultimate.

Software: MATLAB 10.

OBJECTIVE # 1

IMPLEMENTATION OF WAVELET BASED MODIFIED BUYER-SELLER WATERMARKING PROTOCOL (BSWP)

1.1 INTRODUCTION

The rapid growth of computer networks increased use of multimedia data via the internet have resulted in fast and convenient exchange of digital information. Digital watermarking [22] has been proposed, complementing encryption techniques, to establish and prove ownership rights by embedding the seller's information in the redistributed digital content.

The wavelet based modified buyer-seller watermarking protocol is one that combines encryption, digital watermarking, and other techniques to ensure rights protection for both the buyer and the seller in e-commerce. In general the watermark is two types i.e. visible or invisible. A visible watermark typically consists of visible text message or a company logo indicating the ownership of the digital content. In contrast invisible watermarked content appears identical to the original.

Spatial domain techniques are easier to implement, but lacks in robustness, while transforming domain techniques embed the watermark in the host's transform domain, are more sophisticated, robust and getting popularity when compared to spatial domain techniques [23]. The development of spatial domain techniques due to their weakness in robustness is generally not chosen by the researcher and the frequency domain algorithm [24] based on DCT or DWT is the focus of research.

We have assumed that every seller in a transaction has unique watermarking embedded function algorithm in their software and all messages are transferred in a secure manner and digital content is still image. Discrete wavelet transforms (DWT) [25-29] is a signal analytic theory that can localize the signal in spatiotemporal. We have modified the existing algorithm proposed by Corina Nafornita for embedding the watermarks the algorithms used to embed the watermark in the high frequency sub-bands i.e. HL, LH and HH because they show better results in terms of imperceptibility. In our approach we have chosen high frequency selected sub-bands i.e. HL and LH this reduces the area of embedding the watermark leads in great robustness, imperceptibility and minimize the effect of various attacks. We have compared our approach with Corina

Nafornita and shows that the approach contains better result. Embedding of the watermark multiple times into the host image makes the scheme more robust.

1.2 RELATED WORK

The possible solution for e-distribution of digital rights is based on a unique watermark for a transaction between seller and buyer. This has come to be known as buyer seller watermarking protocol. Since its inception in [25] many variants have been proposed. However, DWT [30] has been used more frequently in digital image watermarking due to its time/frequency decomposition characteristics, which resemble to the theoretical models of the human visual system [31]. Ramin Eslami and Hayder Radha propose a new image coding scheme based on the proposed transform, the wavelet-based contourlet transform (WBCT) [32-34]. We have implemented a wavelet based modified buyer seller watermarking protocol to fulfil the design requirements, different from the predecessors, our approach makes improvements in the many aspects such as anonymous communication between buyer and seller, and it supports multi-transaction and dispute resolution and avoid double watermark insertion. The protocol is based on public key encryption standard.

1.3 RESULT ANALYSIS

Here we have shown the various results of wavelet based modified buyer seller watermarking protocol. As we know from the previous section the details of the image such as edges and textures are well confined into the HH, LH, and HL sub-bands of the DWT of the image. We chose only HL_3 and LH_3 sub-bands of the image of the watermarking process. The DWT based algorithm is tested for the various original and watermark images. Some results are given to evaluate the performance of the method. We have calculated PSNR and NCC values for that. The images Lena, Cameramen, Baboon and House are presented in Fig. 1.1. The presented method is implemented using MATLAB10.

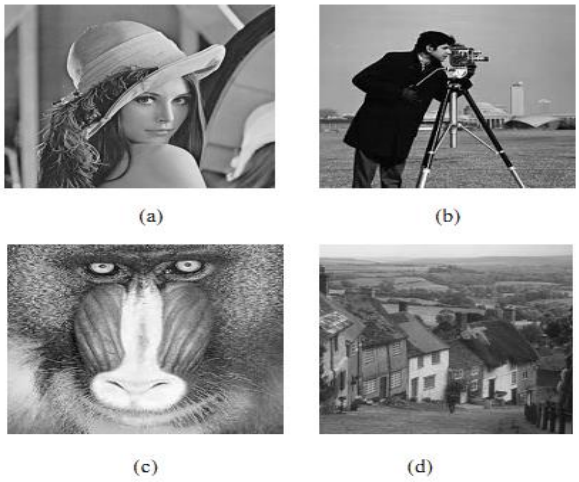


Fig .1.1 *Original images used for simulations: Lena (a), Cameramen (b), Baboon (c) and House (d).*

Table 1PSNR [dB] values as a measure of the noise introduced by the watermark.

PSNR / Image	Our Method	C. Nafornita' Method	Cox's Method
Lena	46.33dB	45.39dB	27.19 dB
Cameraman	44.55 dB	43.35 dB	25.35 dB
Baboon	45.39dB	44.18dB	26.44 dB
House	45.67 dB	45.35 dB	25.75 dB

Table 1

Here we have given the results of our method against the various types of attacks. We have compared our result with the results of the method proposed by Ben Wang [35]. For instance, we have taken only the Lena image for producing our result. So we have taken of 512 × 512 8bit grayscale image Lena image and 128 × 128 8-bit grayscale watermark original binary JUIT logo. The embedding coefficient $\alpha = 0.01$. The robustness are tested under 5 types of attacks i.e. JPEG Compression, Rotation, Gaussian noise, Salt & Peeper noise and median filter. The images with attacks are shown in Figure 1.2.

JAYPEE UNIVERSITY OF INFORMATION TECHNOLOGY
juit
विद्या तत्व ज्योतिसम्
(a) Original Image
(b) Original Binary JUIT logo
(c) Watermarked Image
(d) JPEG Compression (60%)
(e) Rotation (30°)
(f) Rotation (60°)
(g) Gaussian noise at = 0.01
(h) Gaussian noise at = 0.08
(i) Salt & Peeper noise at = 0.01
(j) Salt & Peeper noise at = 0.08
(k) Median Filter at [5 5]
(l) Median Filter at [9 9]

Fig. 1.2 *Images with various types of attacks.*

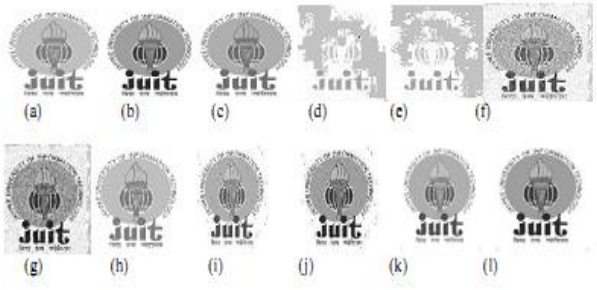


Fig. 1.3 *Watermarks extracted from the attacked Images.*

The watermarks extracted from the images above are shown correspondingly in Figure 1.3. In this a wavelet based modified buyer-seller watermarking protocol (BSWP) is implemented.

OBJECTIVE # 2

ROBUST BUYER-SELLER WATERMARKING PROTOCOL (RBSWP) BASED ON DISCRETE WAVELET TRANSFORM (DWT) AND PRINCIPAL COMPONENT ANALYSIS (PCA)

2.1 INTRODUCTION

Digital image watermarking is a technique that hides a bit of data in a host image for the intention of copyright protection and integrity checking. In digital watermarking some information such as images, audio and video can be embedded in the data in such a way that it is not perceptible to the human eye or by human vision system (HVS) model.

In our protocol we have used wavelets and PCs to provide more security for the buyer and the seller during the transmission of digital content. Our protocol focuses on managing the watermarks means the concern is only watermark generation protocol and watermark insertion protocol. We have ensured that our protocol is more robust compare to other previous proposed protocols because it uses wavelet special properties and principal components PCs. In this paper, the seller provides the watermark embedding operation and sells the watermarked product to the buyer. We have assumed that every seller in a transaction has unique watermarking embedded function algorithm in their software and all messages are transferred in a secure manner and digital content is still image.

In this, the watermark bits are embedding into the maximum coefficient of the PCA block this leads in great robustness. In this algorithm a watermarked image that is a baby image is embedded into certain selected high frequency sub-bands of a 3-level discrete wavelet transform of the original image. Then author have applied Principal Component Analysis (PCA) on these high frequency wavelet coefficients and stored the mean (Ai) and covariance (Ci) of the data onto the first principal component called PCs. After applying principal component analysis (PCA) transformation we have chosen blocks for embedding the watermark. The selection of the blocks are depends by calculating the energy of each block, then we choose only those blocks which contain maximum energy. The watermark bits are embedding into the maximum

coefficient of the PCA block. The extraction procedure of the watermark is same as we embed the watermark.

2.2 BACKGROUND

One of the solutions for e-distribution of digital rights is based on a unique watermark for every transaction between seller and the buyer. We have demonstrated a robust buyer-seller watermarking protocol based on DWT and PCA to fulfil the design requirements, unlike from the predecessors; our approach makes improvements in the many aspects such as anonymous communication between buyer and vendor. The watermarking scheme [39] for embedding and extracting the watermarks is more robust and imperceptible because it uses a hybrid technique.

2.3 RESULT ANALYSIS

In this section author have shown the various results of robust buyer seller watermarking protocol based on DWT and PCA. The details of the image such as edges and textures are well confined into the high frequency sub-bands of the DWT of the image. First, we decomposed the image up to 3 levels, select only HL_3 and LH_3 sub-bands of the DWT image, then watermark is embedded in the principal components of the high frequency wavelet coefficients. We have calculated PSNR and NCC values for that. We use the popular standard test images database of Lena, Peppers, Baboon, and Fruits of size 512 × 512 each is shown in figure 2.1 (a-d) and corresponding watermark image are shown in figure 2.1 (e-h).

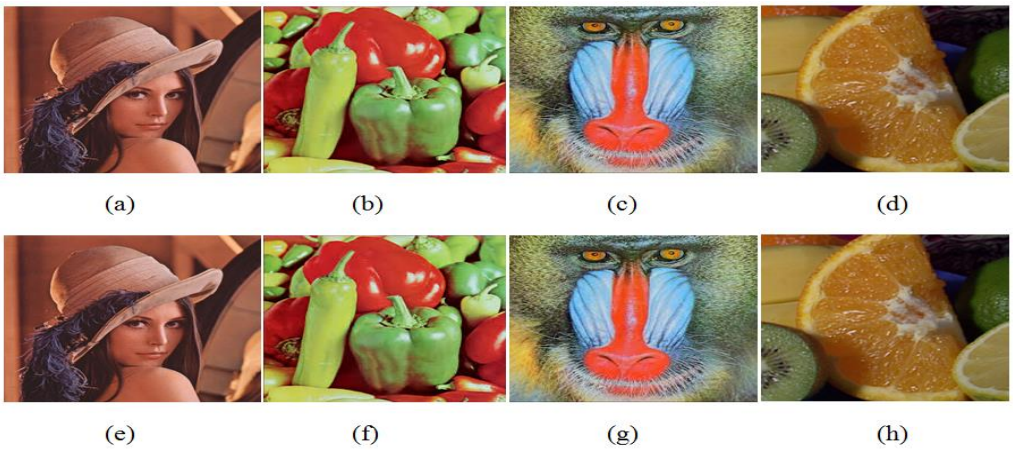


Fig. 2.1 *(a) Lena (b) Peppers (c) Baboon (d) Fruits (e) Watermarked lena (f) Watermarked peppers (g) Watermarked baboon (h) Watermarked fruits*

We have taken the gray-scale watermark of size 256 × 256. This watermark is embedded into Lena, Peppers, Baboon, and Fruits images respectively. The presented method is implemented using MATLAB. We have taken the gray-scale watermark of size 256 × 256. This watermark is embedded into Lena, Peppers, Baboon, and Fruits images respectively. The presented method is implemented using MATLAB. Form 2.1 (e-h) shows the resultant watermarked images and corresponding PSNR values are presented in Table 2. The color watermark was a baby image of different sizes. The Daubechies 10pt wavelet was used to bring about the wavelet coefficients. The following parameters were used, number of resolution levels L = 3, the strength of the watermark $\alpha = 0.1$. The images are first decomposed using DWT then a watermark is embedded in the principal components of the high frequency wavelet coefficients.

Fig. 2.2 *(a) Original watermark (b) Extracted watermark (c) Binary watermark*

Table 2 Peak signal to noise ratio (PSNR) dB for each original color image.

Test color images	Lena	Peppers	Baboon	Fruit
PSNR	43.59	41.68	39.25	38.57

In this, a robust buyer-seller watermarking protocol based on DWT and PCA is shown. The watermarking embedding method that embeds the watermark in coefficients selected in such a way that the visible impact on a human observer is not very high. The method is implemented using 3-level DWT with PCA transform. A gray-scale watermark image has been embedded only the maximum energy blocks were chosen for the embedding procedure. The protocol focuses on managing the watermarks we do not design novel method. Our scheme performs better when compared with existing reporting methods Run et al. Lai et al. Ahahmad et al. and Bhatnager et al. The simulation results have proven that the scheme performs well against JPEG Compression, Rotation, Gaussian Noise, Salt & Pepper Noise and Median Filter.

OBJECTIVE # 3

AN ID-BASED SECURE AND FLEXIBLE BUYER-SELLER WATERMARKING PROTOCOL FOR COPYRIGHT PROTECTION

3.1 INTRODUCTION

The speedy development of internet and e-commerce needs a copyright protection mechanism for multimedia data. Straight off a day's digital watermarking becomes an important technique for protecting the digital rights. The principal object of digital watermarking technique is to retain digital copyright or watermark, embedded into the cover object. The desirable secure digital watermarking scheme is one, which integrates public key cryptosystem and digital watermarking technique for protecting the buyer and seller in a digital content transaction. Digital watermarking techniques uses encrypted domain for embedding and extracting the watermarks. The rapidly growing of the internet encourages some bad usage too, like operations such as transformation, duplication, and redistribution of digital content. With the avail of some software tools, we can easily identify these bad users and redistribution of digital content can also be placed. In general, secure digital watermarking scheme should satisfy the following requirements.

In the history, Hwang et al. introduced a time stamping protocol in 2005. In their protocol, a TTP (trusted third party) was introduced for checking the verification and signing phase. In our suggested protocol, author use same trust model uses by Memon [21] and Lei [36]. The proposed protocol is based on public key infrastructure, arbiter, ID based public key cryptography and digital watermarking scheme. The watermarking scheme involved secret key and digital signature certificate issued by WCA. WCA maintains its own table and keeping the requested IDs of both buyer and seller because it contains a database. Tamper resistance device is used to reduce the overhead on WCA. Now, in the digital signature verification phase someone else can use the WCA public keys to validate that the watermark content that was embedded at a certain time into the digital content. The proposed digital watermarking protocol consists three sub-protocols: the watermark embedding and signing protocol; watermark detecting and verifying protocol; and registration protocol.

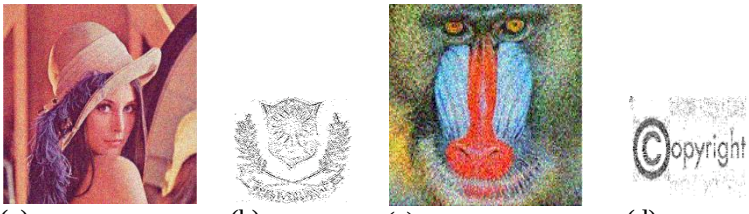
3.2 BACKGROUND

J. Zhang et al. proposed a secure buyer seller watermarking protocol in 2006. The author proposed a secure buyer seller watermarking protocol without the assistance of a TTP in which there are only two participant's seller and buyer. J. Zhang paper is based on the Lei et al. and in this no third party is brought in; therefore, the proposed protocol is more childlike and more dependable than the existing watermarking protocol. J. Zhang protocol resolves the conspiracy problem, piracy tracing problem & customer's right problem. However, there is a drawback in the J. Zhang protocol, i.e. the buyer's assistance is needed to solve the piracy dispute problem.

3.3 RESULT ANALYSIS

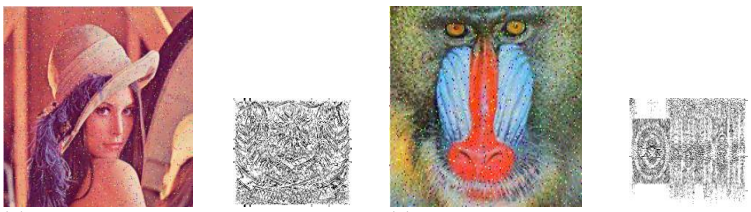
In this section, the security of the proposed ID-based secure and flexible buyer-seller watermarking protocol is analyzed. The security of the proposed protocol depends on the security and robustness of the underlying watermarking embedding and detecting scheme. We have examined the security of our protocol and compare with scheme of [37], [38], [21], [36]. The proposed watermarking protocol is secure for the reason that buyer has no idea about the original digital content X hence, is unable to remove the watermark. Since seller gets no access to the watermarked copy of the digital content X hence, the seller cannot distribute illegal replicas of digital content X. Our proposed protocol solved the problems identified in J. Zhang protocol and problems, which are listed in section 1.

Here, for calculating the robustness of the watermark embedding scheme we have applied several types of attacks to the watermarked images.



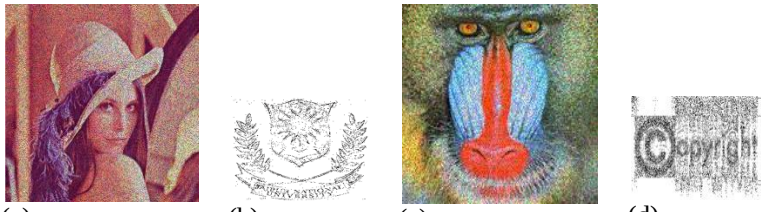
(a) (b) (c) (d)

Fig. 3.1 a) *Watermarked Lena Image after Gaussian Noise at 0.02 b) Extracted Watermark c) Watermarked Baboon Image after Gaussian Noise at 0.02 d) Extracted Watermark.*



(a) (b) (c) (d)

Fig. 3.2 a) *Watermarked Lena Image after Salt & Pepper Noise at 0.02 b) Extracted Watermark c) Watermarked Baboon Image after Salt & Pepper Noise at 0.02 d) Extracted Watermark.*

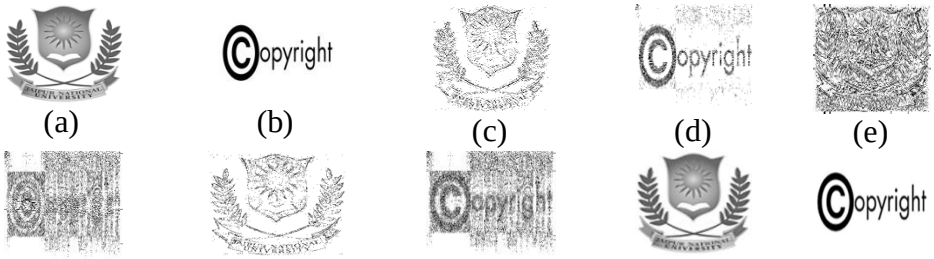


(a) (b) (c) (d)

Fig. 3.3 a) *Watermarked Lena Image after Speckle Noise at 0.03 b) Extracted Watermark c) Watermarked Baboon Image after Speckle Noise at 0.03 d) Extracted Watermark.*

(a) (b) (c) (d)

Fig. 3.4 *a) Watermarked Lena Image after Median Filter at [5 5] b) Extracted Watermark c) Watermarked Baboon Image after Median Filter at [5 5] d) Extracted Watermark.*



(a) (b) (c) (d) (e)

(f) (g) (h) (i) (j)

Fig. 3.5 *Extracted Watermark Images*

In figure 3.1 author have applied Gaussian noise with density of 0.02 to the watermarked Lena and Baboon image, the JNU watermark logo and copyright logo are embedded respectively. The quality of the extracted watermark logos are good with the presence of attacks. To check the quality of these watermark we have calculated correlation coefficient.

Figure 3.2 shows the performance of our scheme against the salt & pepper noise we have applied this noise with density of 0.02 on the Lena and aboon watermarked images then we have extracted the corresponding watermarks.

In figure 3.3 we have applied speckle noise with 0.03 density on Lena and Baboon watermarked images then corresponding watermark are extracted. In this we got good result and watermarks are still extracted. Filtering is the most common attacks on digital images. So we have applied median filter to both watermarked images with filter size M=5 in figure 3.4. Figure 3.5 (a,b) shows the original watermarks and (c,d,e,f,g,h,i,j) shows the extracted watermarks from Lena, and Baboon images. In this, author present an identity-based buyer-seller watermarking protocol which can solve the various problems of the previously published protocol and free from all know attacks. In addition, author make use of a tamper resistance device, which is embedded into seller's computer and reduces the overhead on WCA.

Author also adopt wavelet and principal component analysis based techniques to increase the robustness and imperceptibility of our embedding scheme. The watermark certificate authority will responsible for issuing the digital signature corresponds to ID of the seller. If the problem of multiple ownership occurs, then it is the duty of an arbiter to decide it. The arbiter checks the correctness of data used by the seller, and then the arbiter compares the timestamps for determining the true possessor of the digital content. These changes enable the proposed protocol is really secure, feasible and efficient.

CONCLUSION AND FUTURE WORK

Conclusion

This thesis emphasizes on watermarking embedding and extraction scheme into the buyer-seller watermarking protocol. A buyer-seller watermarking protocol consists four main sub-protocols, i.e. Watermark generation protocol, Watermark insertion protocol, Copyright violator identification protocol and Dispute resolution protocol. Firstly we have emphasized on watermark generation protocol and watermark insertion protocol. Secondly author has worked on cryptosystem with digital watermarking scheme which uses id-based public key cryptography for providing more security to the buyer and seller. In this we also make use of a tamper resistance device to reduce the overhead on WCA as TTP.The last section of the thesis concludes the work and addresses the scope for future enhancements.

In objective first, a robust and efficient watermarking embedding and extraction scheme based on discrete wavelet transform to improve the robustness and imperceptibility of the watermark is proposed. Unlike existing buyer-seller watermarking protocol, this approach uses wavelet based methods for watermark embedding and extraction these methods are more robust. The quality of the watermarked image generated with wavelet based method is better, using the same watermark strength. By embedding the watermark bits into the edges and textures i.e. HL3, HH3, and LH3 sub-bands of the image we make use of the human visual system. It is clarified that the wavelet based transform such as DWT, is better than other transform in terms of imperceptibility, robustness and capacity.

In objective second, the author proposed a lightweight watermarking embedding and extraction scheme as an improved variation of the above scheme which makes use of principle component analysis with wavelets together for further increasing the robustness of the watermark. This protocol uses wavelet transform with principal component analysis and integrates digital watermarking techniques and public key cryptosystem for proving the ownership of digital content. Principal component analysis is used to reduce the correlation coefficient. The method is implemented using 3-level DWT with PCA transform. The method is also image dependant and able to survive under geometric distortion and image processing attacks. PCA is a powerful tool

for analyzing data and finding patterns in it. PCA gives a high compression rate and performance is good when noise is present. It is also used for removing the correlation coefficients amongst the dataset. These aspects make our protocol efficient and robust.

In this author proposed a cryptosystem with digital watermarking scheme which uses id-based public key cryptography for providing more security to the buyer and seller. The suggested protocol uses Id-based public key cryptography and digital watermarking scheme to place the ownership of digital content. Hence, copyright protection is attained. WCA maintains its own table and keeping the requested IDs of both buyer and seller. Hence, it is not required for WCA to participate in each transaction of the digital content between buyer and seller. The suggested protocol is efficient and have adequate security from traditional proposed protocols and suitable for any practical buyer seller watermarking scheme.

This synopsis proposed new methods for embedding and extracting the watermark and increase the robustness and imperceptibility. Results show that the proposed embedding approaches are better than the previously proposed scheme in case of robustness and imperceptibility.

Future Work

In future the work can be done to provide more effective solutions for the identified problems. In addition the presented methods for embedding and extracting the watermark can be tested on other gray-scale image datasets for further establishing their efficacy. The research can further expand by study the effect of others optimization technique. This is designed for public key cryptosystem and the operations of watermark insertion are performed by the seller rather than the certification authority. The protocol has higher efficiency, and it is very safe. The security of this protocol lies on the security and robustness of the encryption standard and different group signature, and technique used in this protocol, which can further be modified and developed to improve the efficiency of the protocol.

References

[1] F.N. Lang, et al, "A self-adaptive image normalization and quaternion PCA based color image watermarking algorithm," Expert Systems with Applications, vol. 39 no. 15, pp. 12046–12060, 2012.

[2] Yin CQ, Li L, Lv AQ, Qu L, "A color image watermarking algorithm based on DWT-SVD,"IEEE Int. Conf. on Automation and Logistics, Jinan, pp. 18-21, 2007.

[3] F. Mintzer, and G. W. Braudaway, "If one watermark is good, are more better?," In Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP '99), vol. 4, Phoenix, Ariz, USA, pp. 2067–2069, 1999.

[4] P. W. Wong, and N. Memon, "Secret and public key image watermarking schemes for image authentication and ownership verification," IEEE Transactions on Image Processing, vol. 10, no. 10, pp. 1593–1601, 2001.

[5] Zeng, P, Cao, Z, Choo, K.R, "An ID-based digital watermarking protocol for copyright protection," Computers and Electrical Engineering vol. 37, pp. 526–531, 2011.

[6] B.-M. Goi, et. al. "Cryptanalysis of Two Anonymous Buyer-Seller Watermarking Protocols and An Improvement for True Anonymity," In Applied Cryptography and Network Security, LNCS 2587, pp. 369–382, 2004.

[7] M. Kuribayashi, and H. Tanaka, "Fingerprinting protocol for images based on additive homomorphic property," IEEE Transactions on Image Processing, vol. 14, no. 12, pp. 2129–2139, 2005.

[8] F. C. Chen, T. Ming, and S. Wei-Zhe, "Buyer-Seller Watermarking Protocols with Off-line Trusted Parties," MUE '07. International Conference on Multimedia and Ubiquitous Engineering, pp. 1035–1040, 2007.

[9] M. Ibrahim, S. H. N. El-Din, and A. F. A. Hegazy, "An effective and secure buyer-seller watermarking protocol," In Third International Symposium on Information Assurance and Security, IAS, pp. 21–28, August, 2007.

[10] S. Katzenbeisser, A. Lemma, M. U. Celik, M. van der Veen, and M. Maas, "A buyer-seller watermarking protocol based on secure embedding," IEEE Trans. Inf. Forensics Security, vol. 3, no. 4, pp. 783–786, December, 2008.

[11] Y. Hu, and J. Zhang, "A secure and efficient buyer-seller watermarking protocol," Journal of Multimedia, vol. 3, no.4, pp.161-168, 2009.

[12] A. Kumar, M. D. Ansari, J. Ali, K. Kumar, "A New Buyer-Seller Watermarking Protocol with Discrete Cosine Transform," in CNC CCIS 142, Springer-Verlag Berlin Heidelberg, pp. 468–471, 2011.

[13] A. Kumar, V. Tyagi, M. D. Ansari, and K. Kumar, "A Practical Buyer-Seller Watermarking Protocol based on Discrete Wavelet Transform, International Journal of Computer Applications, pp. 46-51. 2011.

[14] J. Rial, Balasch, and B. Preneel., "A privacy-preserving buyer seller watermarking protocol based on priced oblivious transfer," IEEE Transactions on Information Forensics and Security, pp. 202–212, 2011.

[15] X. Cui, G. Sheng, F. Li, and X. Liu, "An Efficient and Impartial Buyer-Seller Watermarking Protocol," Journal of Communications, vol. 10, no. 5, pp. 339-344, 2015.

[16] C. de Carvalho J, and Sequeira L, "Buyer-seller conflict and cooperation in marketing channels: port wine distribution," International Journal of Wine Research, 2013.

[17] C. L. Chena, C.C. Chenb, D. K. Lic, and P.Y. Chend, "A Verifiable and Secret Buyer–Seller Watermarking Protocol," IETE Technical Review Vol. 32, no. 2, pp. 104-113, 2015.

[18] J. Q. Xie, Q. Xie, L. J. Tian, "A Buyer-Seller Digital Watermarking Protocol without Third Party Authorization", Advanced Engineering Forum, Vols. 6-7, pp. 452-458, 2012.

[19] L. S. Hwan, K. S. Geun, and K. K. Ryong, "Mobile 3D Secure Transmission Based on Anonymous Buyer-Seller Watermarking Protocol," Recent Advances in Communications and Networking Technology," Vol. 3, no. 1, pp. 33-43, July 2014.

[20] M. Deng, and B. Preneel, "On Secure and Anonymous Buyer-Seller Watermarking Protocol," Third International Conference on Internet and Web Applications and Services, pp. 524-529. June, 2008.

[21] N.D. Memon, P.W. Wong, "A buyer-seller watermarking protocol," IEEE Transactions on Image Processing, 2001.

[22] J. Cox, J. Kilian and T. Shamoon, "Secure spread spectrum watermaking for multimedia," IEEE Transaction of Image Processing, vol. 6 no. 12, pp. 1673-1687, 1997.

[23] V. Potdar, S. Han, and E. Chang, "A survey of digital image watermarking techniques, in Proc. of the IEEE International Conference on Industrial Informatics," pp. 709-716, 2005.

[24] C. Chan, and L. Cheng, "Hiding data in Images by simple LSB substitution," Pattern Recognition, vol. 37, no. 3, pp. 469-474, 2004.

[25] J.C. Liu, C. H. Lin, and L.C. Kuo, "A robust full band image watermarking scheme," Proceedings on IEEE, 2006.

[26] X. G. Xia, C. G. Boncelet, and G. R. Arce, "A multiresolution watermark for digital images," Image Processing Proceedings. International Conference, vol. 1 pp. 548–551, 1997.

[27] M. Kutter, S. K. Bhattacharjee, and T. Ebrahimi, "Towards second generation watermarking scheme, Image Processing, (ICIP) Proceedings, vol. 1, pp. 320–323, 1999.

[28] A. A. Haj, "Combined DWT-DCT digital image watermarking," Journal of computer science, vol. 3, no .9, pp. 740-746. 2007.

[29] S. A. Kasmani, and A. N. Nilchi, "A new robust digital image watermarking technique based on Joint DWT-DCT transformation," Third International Conference on Convergence and Hybrid Information Technology, pp. 42-54. 2008.

[30] P. Tay, and J. Havlicek, "Image watermarking using wavelets," in Proc. of the IEEE Midwest Symposium on Circuits and Systems, pp. 258-261. 2002.

[31] R. Wolfgang, C. Podilchuk, and E. Delp, "Perceptual watermarks for digital images and video," Proc. of the IEEE, vol. 87, no. 7, pp. 1108-1126. 1999.

[32] R. Eslami, and H. Radha, "Waveletbased contourlet transform and its application to image coding," in Proceedings of the IEEE International Conference on Image Processing (ICIP'04), IEEE Signal Processing Society, pp. 3189–3192, 2004.

[33] P. kumhom, K. chamnongthail, "Image watermarking based on wavelet packet transform with best tree," Ecti Transactions on Electrical-eng, Electronics, and Communications, vol 2, no. 1, pp. 23-35. 2004.

[34] L. Qiao, and K. Nahrstedt, "Watermarking Schemes and Protocols for Protecting Rightful Ownership and Customer's Rights," Journal of Visual Communication and Image Representation, vol. 9, no. 3, pp. 194–210, 1998.

[35] J. Wang, Q. Ding, X. Liao, and C. Liu, "An image watermarking algorithm based on DWT DCT and SVD," Proceeding of ICNIDC, pp. 1034-1038, 2009.

[36] C.-L. Lei, P.-L. Yu, P.-L. Tsai, M.-H. Chan, "An efficient and anonymous buyer-seller watermarking protocol," Transactions on Image Processing, 2004.

[37] J. Zhang, W. Kou, K. Fan, "Secure buyer-seller watermarking protocol," IEEE Proceedings Information Security, 2006.

[38] Choi, J.-G, Sakurai, K, Park, J.-H, "Does it need trusted third party? Design of buyerseller watermarking protocol without trusted third party," In: Zhou, J., Yung, M., Han, Y.(eds.) ACNS, LNCS, vol. 2846, Springer, Heidelberg, pp. 265–279, 2003.

[39] Ju, H.S, Kim, H.-J, Lee, D.-H, Lim, J.-I, "An anonymous buyer-seller watermarking protocol with anonymity control," In: Lee, P.J., Lim, C.H. (eds.) ICISC, LNCS, vol. 2587, Springer, Heidelberg, pp. 421–432, 2003.

LIST OF PUBLICATIONS

5.1 Journal Publications

[1] A. Kumar, S.P. Ghrera, and V. Tyagi, "An ID-based secure and flexible buyer-seller watermarking protocol for proving ownership of digital content," Journal of Science & Technology. **[SCOPUS indexed]. (Accepted)**

[2] A. Kumar, S.P. Ghrera, and V. Tyagi, "Modified Buyer Seller Watermarking Protocol based on Discrete Wavelet Transform and Principal Component Analysis," Indian Journal of Science and Technology, Vol. 8, no. 35, pp. 1-9, 2015. **[SCOPUS indexed].** http://dx.doi.org/10.17485/ijst/2015/v8i35/47258

[3] A. Kumar, S.P. Ghrera, and V. Tyagi, "Implementation of Wavelet Based Modified Buyer-Seller Watermarking Protocol," WSEAS Transactions on Signal Processing ,Vol. 10, pp. 212-220, April 2014. [SCOPUS indexed]. http://www.wseas.org/multimedia/journals/signal/2014/a025714-226.pdf

[4] A. Kumar, S.P. Ghrera, and V. Tyagi, "Survey of Buyer-Seller Watermarking Protocol," International Journal of Technology & Management, vol. 6, pp. 51-65, September 2013.

5.2 Conference Proceedings

[1] A. Kumar, S.P. Ghrera, and V. Tyagi, "A Comparison of Buyer-Seller Watermarking Protocol (BSWP) Based On Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT)," Computer Society of India (CSI) Vol. 1. pp. 401-408, Springer International Publishing, 2015. **[SCOPUS indexed].** http://dx.doi.org/10.1007/978-3-319-13728-5_45

[2] A. Kumar, S.P. Ghrera, and V. Tyagi, "A new and efficient buyer-seller digital watermarking protocol using Identity based technique for copyright protection," International Conference on Image Information Processing (ICIIP -2015) proceedings IEEE Computer Society Press in IEEE Explore, pp. 531-535, 21-24 Dec 2015. **[SCOPUS indexed IEEE Explore].** https://www.computer.org/csdl/proceedings/iciip/2015/0148/00/07414830-abs.html

[3] A. Kumar, S.P. Ghrera, and V. Tyagi, "A lightweight buyer-seller watermarking protocol based on composite signal representation and time-stamping for multimedia data distribution." in International Conference on Engineering and Material Sciences (ICEMS-2016). **[Indexed in Scopus, and published in SCIENCE DIRECT, Communicated].**